Google Scholar BETA

Web Images Video News Maps more »

"round function" with dummy with block cipher Search

Advanced Scholar Search
Scholar Preferences
Scholar Help

The following words are very common and were not included in your search: **with with**. [details]

Scholar **All articles - Recent articles** Results **21 - 30** of about **31** for **"round function" with dummy**

All Results
M Jacob
J Kelsey
D Boneh
E Felten
B Schneier

[BOOK] Information Security and Cryptology--Icisc'99: second international conference, Seoul, Korea, ...
JS Song - 2000 - books.google.com
... Feistel scheme in which the sth **round function** is F ... by replacing repeated quer -ies by **dummy** queries ... MAC construction which transforms a **block cipher** function C ...
Related Articles - Web Search - Library Search

Design Challenges for a Differential-Power-Analysis Aware GALS-based AES Crypto ASIC - all 2 versions »
FK Gürkaynak, S Oetiker, H Kaeslin, N Felber, W ... - Electronic Notes in Theoretical Computer Science, 2006 - Elsevier
... Aes consists of a **round function** composed of four main op- erations: ... A special **block** is used to interface with a syn ... Data I/O MixColumns 2 **Dummy** Operation ...
Related Articles - Web Search

Watermark detector - all 5 versions »
PJ Lenoir, JC Talstra, JPMG Linnartz - US Patent 6,671,806, 2003 - Google Patents
... by the 60 detector through zeroes or **dummy** data before ... **cipher** which operates with 96 bits data **block** and 96 ... 3-Way has a **round function** which is recommended to ...
Related Articles - Web Search

A Network-based Asynchronous Architecture for Cryptographic Devices - all 3 versions »
L Spadavecchia - 2006 - banshee.lib.ed.ac.uk
... 11 2.2 The DES **round function**. . . ... 225 C.2 Rijndael: Shift offsets for different **block** lengths . . ... noticed that the power consumption of these **dummy** Page 21. 3 ...
Related Articles - View as HTML - Web Search

Security on FPGAs: State-of-the-art implementations and attacks - all 5 versions »
T Wollinger, J Guajardo, C Paar - ACM Transactions on Embedded Computing Systems (TECS), 2004 - portal.acm.org
... 1981]). It is also attractive to customize **block cipher** such as DES or AES with proprietary S-boxes for certain appli- cations. Further ...
Cited by 16 - Related Articles - Web Search

Design and Analysis of RC4-like Stream Ciphers - all 8 versions »
M McKague - uwspace.uwaterloo.ca
... 30 4.1.1 Feedback in **Block Ciphers** . . . . . 31 4.1.2 Modelling with Finite State Machines . . . .
Related Articles - View as HTML - Web Search

AA MMooddeell ttoo PPrrootteecctt MMoobbiillee AAggeennttss ffrroomm

Patents

Patents **1 - 3** on **round with dummy with block cipher**. (**0.14** seconds)

Secure processor with external memory using **block** chaining and **block** re-ordering
US Pat. 6061449 - Filed Oct 10, 1997 - General Instrument Corporation
For **cipher block** chaining, this has the advantage of not requiring more than ...
Dummy data may also be communicated between the storage device 110 and the ...

Method of and apparatus for selective resynchronization in a digital cellular communications system
US Pat. 5546464 - Filed Sep 16, 1994 - Ericsson Inc.
The mobile station may transmit a **dummy** burst lo announce its presence on the
... station enables the **cipher** with the value received in the **block** counter ...

Bitstream for configuring a PLD with encrypted design data
US Pat. 7117373 - Filed Nov 28, 2000 - XILINX, Inc.
3 shows a **block** diagram of an FPGA (a type of 40 PLD to be partly ... 5a, after
a **dummy** word (a constant high embodiment, bus 26 is present and bus 25 is ...